



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/763,079	01/22/2004	Daniel Brokenshire	AUS920030972US1	6481
50170 7590 02/25/2011				
IBM CORP. (WIP)				
c/o WALDER INTELLECTUAL PROPERTY LAW, P.C.				
17330 PRESTON ROAD				
SUITE 100B				
DALLAS, TX 75252				
EXAMINER				
ANWAR, MACEEH				
ART UNIT		PAPER NUMBER		
2451				
MAIL DATE		DELIVERY MODE		
02/25/2011		PAPER		

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

---

BEFORE THE BOARD OF PATENT APPEALS  
AND INTERFERENCES

---

*Ex parte* DANIEL BROKENSHIRE HARM PETER HOFSTEE,  
and MOHAMMAD PEYRAVIAN

---

Appeal 2009-006207  
Application 10/763,079  
Technology Center 2400

---

Before JOSEPH L. DIXON, ST. JOHN COURTENAY III, and  
THU A. DANG, *Administrative Patent Judges*.

COURTENAY, *Administrative Patent Judge*.

DECISION ON APPEAL<sup>1</sup>

STATEMENT OF THE CASE

---

<sup>1</sup> The two-month time period for filing an appeal or commencing a civil action, as recited in 37 C.F.R. § 1.304, or for filing a request for rehearing, as recited in 37 C.F.R. § 41.52, begins to run from the “MAIL DATE” (paper delivery mode) or the “NOTIFICATION DATE” (electronic delivery mode) shown on the PTOL-90A cover letter attached to this decision.

This is an appeal under 35 U.S.C. § 134(a) from the Examiner's final rejection of claims 1-15 and 18-23. Claims 16 and 17 have been cancelled. We have jurisdiction under 35 U.S.C. § 6(b).

We Affirm-in-part.

### *Invention*

Appellants' invention relates generally to the field of secure electronic communications. More particularly, the invention on appeal is directed to a unidirectional protocol for message masking and validation using a hash function. (Spec. 1).

### *Representative Claim*

1. A system in a message source for secure communication, comprising:
  - a random value generator configured to generate a random value;
  - a message validation code generator coupled to the random value generator and configured to generate a message validation code based on a predetermined key, a message, and the random value;
  - a one-time pad generator coupled to the random number generator and configured to generate a one-time pad based on the random value and the predetermined key;
  - a masked message generator coupled to the one-time pad generator and configured to generate a masked message based on the one-time pad and the message, and
  - a transmitter configured to transmit a secure message that comprises the random value, the masked message, and the message validation code to a message target,

wherein the message target is configured to unmask the masked message to form the message and validate the message using the message validation code.

*Examiner's Rejections*

1. Claims 22 and 23 stand rejected under 35 U.S.C. § 112, first paragraph, as failing to comply with the enablement requirement.
2. Claims 22 and 23 stand rejected under 35 U.S.C. § 101 as being directed to nonstatutory subject matter.
3. Claims 1-15 and 18-23 stand rejected under 35 U.S.C. § 102(e) as being anticipated by Shrader (U.S. Patent No. 6,914,985).

*112 1<sup>st</sup> paragraph enablement rejection*

Claims 22 and 23

The Examiner contends that Appellants' Specification fails to sufficiently point out computer readable media so as to enable one skilled in the art to make and use the claimed invention. (Ans. 3).

The "enablement requirement is satisfied when one skilled in the art, after reading the specification, could practice the claimed invention without undue experimentation." *AK Steel Corp. v. Sollac*, 344 F.3d 1234, 1244 (Fed. Cir. 2003) (citation omitted). Whether undue experimentation is required is a conclusion reached by weighing several underlying factual inquiries. *In re Wands*, 858 F.2d 731, 736 (Fed. Cir. 1988). A "specification need not disclose what is well known in the art." *Lindemann Maschinenfabrik GmbH v. American Hoist & Derrick Co.*, 730 F.2d 1452, 1463 (Fed. Cir. 1984). However, this "is merely a rule of supplementation, not a substitute for a basic enabling disclosure." *Genentech, Inc. v. Novo*

*Nordisk, A/S*, 108 F.3d 1361, 1366 (Fed. Cir. 1997). It means that the omission of minor details does not cause a specification to fail to meet the enablement requirement. *Id.* It is the specification, not the knowledge of one skilled in the art, that must supply the novel aspects of an invention in order to constitute adequate enablement. *Id.*

Here, we observe that Appellants' Specification discloses at least one embodiment of a medium as an integrated circuit coded to perform functions. (Spec. 3, ll. 14-15; *see also* App. Br. 7). Therefore, we are satisfied that one skilled in the art could practice the claimed invention after reading the Specification without undue experimentation. Accordingly, we reverse the Examiner's rejection of claims 22 and 23 under § 112, first paragraph.

### *§101 rejection*

#### Claims 22 and 23

Regarding the Examiner's §101 rejection of computer readable medium claims 22 and 23, we note that "[t]he four categories [of § 101] together describe the exclusive reach of patentable subject matter. If a claim covers material not found in any of the four statutory categories, that claim falls outside the plainly expressed scope of § 101 even if the subject matter is otherwise new and useful." *In re Nuijten*, 500 F.3d 1346, 1354 (Fed. Cir. 2007).

Here, we particularly observe that Appellants' Specification expressly guides the artisan that "[t]he particular embodiments disclosed above are illustrative only . . . ." (Spec. 10, ll. 11-12). Therefore, consistent with Appellants' Specification, we broadly but reasonably construe the scope of

the claimed “computer program product having a computer readable medium” (claims 22 and 23) as encompassing both statutory (i.e., non-transitory tangible media) and transitory non-statutory propagating signals. Because the scope of claims 22 and 23 covers both statutory and non-statutory embodiments,<sup>2</sup> claims 22 and 23 fall outside the plainly expressed scope of 35 U.S.C. § 101.

Additionally, see the Feb. 23, 2010 “Subject Matter Eligibility of Computer Readable Media” policy statement by PTO Director David J. Kappos:

The United States Patent and Trademark Office (USPTO) is obliged to give claims their broadest reasonable interpretation consistent with the specification during proceedings before the USPTO. *See In re Zletz*, 893 F.2d 319 (Fed. Cir. 1989) (during patent examination the pending claims must be interpreted as broadly as their terms reasonably allow). The broadest reasonable interpretation of a claim drawn to a computer readable medium (also called machine readable medium and other such variations) typically covers forms of non-transitory tangible media and transitory propagating signals per se in view of the ordinary and customary meaning of computer readable media, particularly when the specification is silent. *See* MPEP 2111.01. When the broadest reasonable interpretation of a claim covers a signal per se, the claim must be rejected under 35 U.S.C. § 101 as covering non-statutory subject matter. *See In re Nuijten*, 500 F.3d 1346, 1356-57 (Fed. Cir. 2007) (transitory embodiments are not directed to statutory

---

<sup>2</sup> e.g., We conclude that a wireless transmission (computer program product) having a signal or carrier wave (computer readable medium) with computer program data modulated thereon (embedded) is a non-statutory embodiment within the broad scope of Appellants’ claims 22 and 23. .

subject matter) and *Interim Examination Instructions for Evaluating Subject Matter Eligibility Under 35 U.S.C. § 101*, Aug. 24, 2009; p. 2.

1351 OG 212, Feb. 23, 2010 (available at <http://www.uspto.gov/web/offices/com/sol/og/2010/week08/TOC.htm#null>)

For the aforementioned reasons, we sustain the Examiner's rejection of claims 22 and 23 as being directed to non-statutory subject matter under 35 U.S.C. § 101.

*§ 102 rejection*

ISSUE

Based upon our review of the administrative record, we have determined that the following issue is dispositive in this appeal regarding the Examiner's anticipation rejection of independent claims 1, 7, 12, 18, 22, and 23:

Under §102, did the Examiner err in finding that Shrader discloses a message validation code that is: (1) generated based on a predetermined key, a message, and a random value, and is *transmitted as part of the secure message*, within the meaning of the commensurate limitations recited in independent claims 1, 12, 22, and 23, and (2), where the *message validation code is received as part of the secure message*, within the meaning of the commensurate limitations recited in independent claims 7 and 18, and (3), where a one-time pad is generated based on the random value and the predetermined key, as recited in commensurate form within each independent claim on appeal?

### FINDINGS OF FACT

1. Shrader describes generating at random a content-encryption key for a particular content-encryption algorithm and also that content is encrypted with the content-encryption key. (Col. 11, ll. 46-47; 65-67).
2. Shrader describes validation of an “EnvelopedData” object containing encrypted content when the “EnvelopedData” object is imported to or exported from the “EnvelopedData Interface Utility” shown in Fig. 3. (Col. 13, ll. 57-67).
3. Shrader describes that content is encrypted with the content-encryption key where the content-encryption may require that the content be padded to a multiple of some block size. (Col. 11, ll. 65-67).

### ANALYSIS

After considering the evidence before us, and the respective arguments on both sides, we agree with Appellants that Shrader is not an anticipatory reference for essentially the same reasons argued in the Brief (pp. 13-14 and 16).

At the outset, we observe that the Examiner has mapped portions of the aforementioned disputed limitations<sup>3</sup> of each independent claim on appeal to a general discussion of digital signatures and public and private keys found in the “Background of the Invention” section of the reference

---

<sup>3</sup> See ISSUE statement *supra*.



(Shrader, col. 1, ll. 27-43; Ans. 4). The Examiner has also mapped at least part of the disputed message validation code generator to a general discussion of authentication, also found in the Background section of Shrader. (Col. 2, ll. 19-29).

The Examiner additionally relies on Shrader's Figures 3, 4C and 7, and column 13 (lines 57-67) which describes the validation of an "EnvelopedData" object that contains encrypted content. (FF 2; Ans. 4). As for the disputed random value, the Examiner relies on Shrader's description of generating at random a content-encryption key for a particular content-encryption algorithm, and also Shrader's description of content that is encrypted using the content-encryption key. (FF 1; Ans. 5).

Because the Examiner paints with a broad brush in making the anticipation rejection, we are left to speculate as to the precise details of how each disputed claim limitation is expressly or inherently described within the disparate portions of the Shrader reference relied on by the Examiner. We note that the Board is a reviewing body and not a place of initial examination.<sup>4</sup> Moreover, the requirements of § 102 essentially require a one-for-one mapping of each argued limitation to the corresponding portion of the reference, in a manner corresponding to the claimed arrangement, which the Examiner must identify with particularity.

Even if we assume *arguendo* (without deciding) that Shrader describes the disputed message validation code (i.e., a digital signature as proffered by the Examiner, Ans. 15, ¶ 2) that is generated based on a

---

<sup>4</sup> See 35 U.S.C. §6(b) ("The Board of Patent Appeals and Interferences shall, on written appeal of an applicant, review adverse decisions of examiners upon applications for patents . . .").

predetermined key, a message, and a random value (used to generate the key, FF 1), we do not find, nor has the Examiner established, that Shrader generates a one-time pad based on the random value and the predetermined key, as required by the language of each independent claim before us on appeal.

Although Shrader describes that content is encrypted with the content-encryption key where the content-encryption *may require the content be padded to a multiple of some block size* (FF 3), we conclude that the Examiner's reading of the claim term "one-time pad" is unreasonable, overly broad, and inconsistent with Appellants' Specification which describes a one-time pad as a special type of "cipher in which both the sender and recipient each have a copy of the same encryption code, which is used only once and then discarded." (Spec. 4).

While we cannot read these limitations from the Specification into the claim, we note that the term "one-time pad" (OTP) is an established term of art in the field of cryptography. See e.g., U.S. Pat. 6,868,495, "One-time pad Encryption key Distribution," filed July 21, 2000. Because Appellants' usage in the claims is in accordance with the plain meaning of this term, we conclude that the Examiner's reading of "one-time pad" is unreasonably broad under the broadest reasonable interpretation consistent with the Specification as it would have been interpreted by one of ordinary skill in the art.<sup>5</sup>

---

<sup>5</sup> During *ex parte* prosecution, the Patent & Trademark Office (PTO) determines the scope of the claims by giving the language "their broadest reasonable construction 'in light of the specification as it would be interpreted by one of ordinary skill in the art.'" *Phillips*, 415 F.3d 1303 1316 (Fed. Cir. 2005), *quoting In re Am. Acad. of Sci. Tech. Ctr.*, 367 F.3d 1359,

Moreover, the Examiner has failed to respond to this point of argument (as raised by Appellants, App. Br. 14-15) in the “Response to Arguments” section of the Answer (pp. 14-16). Without a substantive, persuasive response to Appellants’ argument from the Examiner, we find the weight of the evidence before us supports Appellants’ position with respect to the anticipation rejection of each independent claim. “[A]bsence from the reference of any claimed element negates anticipation.” *Kloster Speedsteel AB v. Crucible, Inc.*, 793 F.2d 1565, 1571 (Fed. Cir. 1986).

For essentially the same reasons argued by Appellants in the Brief, as further discussed above, on this record we cannot affirm the Examiner’s anticipation rejection of each independent claim on appeal. Because we reverse the anticipation rejection for each independent claim, we also reverse the Examiner’s anticipation rejection of each associated dependent claim.

#### DECISION

We reverse the rejection of claims 22 and 23 under 35 U.S.C. § 112, first paragraph, for failing to comply with the enablement requirement.

We affirm the 35 U.S.C. § 101 rejection of claims 22 and 23.

We reverse the 35 U.S.C § 102 rejection of claims 1-15 and 18-23.

---

1364 (Fed. Cir. 2004); see also *In re Morris*, 127 F.3d 1048, 1054 (Fed. Cir. 1997).

Appeal 2009-006207  
Application 10/763,079

No time period for taking any subsequent action in connection with this appeal may be extended under 37 C.F.R. § 1.136(a).

ORDER  
AFFIRMED-IN-PART

pgc

IBM CORP. (WIP)  
c/o WALDER INTELLECTUAL PROPERTY LAW, P.C.  
17330 PRESTON ROAD  
SUITE 100B  
DALLAS, TX 75252